# Round-up of recent changes to US state data breach laws

While most US state data breach notification laws have similar aspects, there are also notable differences. By **Caleb Skeath** and **Brooke Kahn** of Covington & Burling LLP.

Over the past several months, many states, including Illinois, New York, Texas, and Washington, have passed significant amendments to their state data breach notification laws that will expand the scope of notification obligations under these laws in the event of a breach. Currently, most state data breach notification laws only require notification of residents (and possibly state regulators or others) following a "breach," usually defined as unauthorized access to or acquisition of personally identifiable information (PII). PII, in turn, is often defined by state law as a state resident's name along with a Social Security number, driver's license or state identification card number, or a financial account, debit, or credit card number with any required security code, access code, or password to access a financial account. The recent changes to state data breach notification laws expanded the categories of PII that may trigger notification obligations if breached, imposed new requirements to notify regulators (in addition to affected individuals) in the event of a breach, and implemented specific timing requirements for how soon after a breach individuals and regulators must be notified, among other changes. These changes are summarized in additional detail below, followed by a few additional thoughts on what these actions may mean for future legislative action regarding data breach notification at the state or federal level.

## Summary of changes

**Arkansas:** Following the entry into force of H.B. 1943[1], the definition of PII under Arkansas' data breach notification law has expanded to include certain biometric data of Arkansas residents when disclosed along with a resident's name. As a result of this change, entities might now be required to provide notice in the event of a breach of this information. Entities will also now be required to notify the state Attorney General following certain breaches. Such notifications will need to occur within 45 days, but will only be required if a breach affects more than 1,000 individuals.

**California:** California recently enacted A.B. 1130[2], which will take effect on 1 January 2020. The bill will expand the definition of PII in the state's data breach notification law to include a resident's name along with certain biometric data, a tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify an individual's identity. For breaches involving biometric data, this bill will also permit – but will not require – businesses to provide instructions on how to notify other entities that may have used the same type of data as an authenticator, so that those entities will no longer rely on the data for authentication purposes.

**Illinois:** Once recently-passed S.B. 1624[3] enters into force on 1 January 2020, entities will be required to notify the Illinois Attorney General if the entity provides notice of a breach to more than 500 Illinois residents. This change will significantly expand regulatory notification obligations under the law, as the current version of the Illinois data breach notification law only requires notification to the Illinois Attorney General in limited circumstances for certain entities subject to and compliant with HIPAA.

**Maine:** L.D. 696[4] recently amended Maine's data breach notification law to require notification to affected residents within 30 days after an entity becomes aware of a breach of PII. The previous version of the law did not include a specific time frame for such notifications, although it did state that such notifications must be made as expediently as possible and without unreasonable delay.

**New Jersey:** Following the entry into force of S.B. 52[5], the definition of PII under New Jersey's data breach notification law has expanded to include a resident's name along with credentials for accessing an online account. Previously, the law only defined PII to include a resident's name along with a Social Security number, driver's license or state identification card number, or certain financial account or credit/debit card information.

**New York:** S.B. 5775B[6], which went into effect on 23 October 2019, included significant amendments to New York's data breach notification law. These amendments have expanded the law's definition of PII to also include online account credentials, as well as the following types of data when disclosed with an individual's name: (1) certain biometric data; or (2) a financial account, credit, or debit card number without a security code, access code, or password, if it could be used to access a financial account. In addition, while the previous New York law defined a "breach" to only include unauthorized acquisition of PII, the amendments broadened this definition to also include unauthorized access to PII, potentially expanding the types of breaches that may require notification. While these changes may broaden the scope of the law's applicability, the amendments have also introduced new safe harbors for entities that provide notice to affected individuals in accordance with the Gramm Leach Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), the New York Department of Financial Services cybersecurity regulations (NYS DFS), or other federal or New York state data security rules or regulations.

**Oregon:** As of 1 January 2020, amendments to the state's data breach notification law pursuant to S.B. 684[7] will expand the types of PII covered by the law, and therefore potentially requiring notification in the event of a breach, to include a username or identifying information "for the purpose of permitting

 

access to the consumer's account, together with any other method necessary to authenticate." The amendments will also impose additional obligations on "vendors" who maintain, store, access, manage, or process PII on behalf of "covered entities," including obligations to notify the state Attorney General directly under certain circumstances. (Under the current version of the law, an entity that maintains or possesses PII on behalf of another entity is only required to notify that entity of the breach.)

**Texas:** The state's data breach notification law currently requires notification of individuals as expediently as possible and without unreasonable delay, but without a specific required time frame, and does not require notice to regulators following a breach. Amendments to the state's data breach notification law pursuant to H.B. 4390[8], which will enter into force on 1 January 2020, will require notification to affected individuals within 60 days. Entities will also be required to notify the state Attorney General within 60 days if a breach involves more than 250 residents.

**Virginia:** H.B. 2396[9] has expanded the definition of PII under the state's data breach notification law to include a passport number or military identification number when disclosed with an individual's name. As a result of these amendments, a breach involving these categories of PII may now require notification to individuals and the Virginia Attorney General.

**Washington:** H.B. 1071[10] will implement significant changes to the state's data breach notification law once it enters into force on 1 March 2020. The bill will expand the law's definition of PII – and, therefore, the types of information potentially requiring notice if breached – to include (1) online account credentials, as well as (2) other data elements when disclosed with an individual's name, such as dates of birth, private keys, certain biometric data, medical or health insurance information, or student, military, or passport identification numbers. While the current law requires notice to residents (and the state Attorney General, if more than 500 residents are notified) within 45 days after a breach is discovered, the amendments will shorten this time frame to 30 days.

In addition to changes to generally applicable state data breach notification laws, several states have also recently passed sector-specific breach notification laws. Building on recent trends, six additional jurisdictions (Alabama[11], Connecticut[12], Delaware[13], Maryland[14], Mississippi[15], and New Hampshire[16]) have recently passed breach notification laws aimed at state-licensed insurance entities that, in addition to other requirements, may require notification to certain state regulators within as little as three days. Illinois[17] and Nevada[18], meanwhile, have recently passed laws that will impose breach notification requirements on various providers of educational services, including operators of educational websites and applications.

## The future of data breach legislation

As evidenced by the significant amount of legislative activity seen in recent months related to data breach notification laws, states are continuing to enhance their cybersecurity and breach notification laws in the absence of comprehensive federal legislation regulating these areas. All 50 US states have enacted their own generally-applicable data breach notification laws, and recent updates to these laws have indicated a desire among state legislatures to require quicker notifications for broader categories of PII to keep pace with the increasing risks posed by data breaches. For example, several recent amendments have updated state law definitions of PII to include information that can be used to authenticate or identify an individual, such as official identification numbers, online account credentials, or biometric data, which is increasingly used by businesses for authentication purposes. New requirements in several states regarding the timing of breach notices to impacted individuals indicates an interest in ensuring that consumers receive information about a breach in a timely manner, while new requirements to notify state regulators following a breach could facilitate increased oversight of data security and breach notification practices by these regulators.

Given the current patchwork of state data breach notification laws that can vary significantly from one state to the next, the prospect of federal legislation could provide greater certainty for businesses and remove burdens associated with complying with different state laws. However, efforts to pass a federal data breach notification bill have encountered differing perspectives on key issues among various stakeholders, including the degree to which it might preempt state law. While discussions continue at the federal level to identify an approach that could serve as the foundation for a federal data breach notification bill, more activity in this space at the state level appears to be likely, and businesses should continue to monitor for updates to state laws and ensure compliance with any applicable requirements.

**AUTHORS**

Caleb Skeath and Brooke Kahn are Associates at Covington & Burling LLP.
Emails: cskeath@cov.com
bkahn@cov.com

**REFERENCES**

1 www.arkleg.state.ar.us/assembly/2019/2019R/Acts/Act1030.pdf
2 leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1130
3 www.ilga.gov/legislation/BillStatus.asp?DocTypeID=SB&DocNum=1624&GAID=15&SessionID=108&LegID=118713
4 legislature.maine.gov/legis/bills/display_ps.asp?LD=696&snum=129
5 www.njleg.state.nj.us/bills/BillView.asp?BillNumber=S52
6 www.nysenate.gov/legislation/bills/2019/s5575
7 olis.leg.state.or.us/liz/2019R1/Measures/Overview/SB684
8 capitol.texas.gov/BillLookup/History.aspx?LegSess=86R&Bill=HB4390
9 lis.virginia.gov/cgi-bin/legp604.exe?191+sum+HB2396
10 app.leg.wa.gov/billsummary?BillNumber=1071&Year=2019
11 arc-sos.state.al.us/PAC/SOSACPDF.001/A0013015.PDF
12 www.cga.ct.gov/2019/ACT/pa/pdf/2019PA-00117-R00HB-07424-PA.pdf
13 legis.delaware.gov/BillDetail/47568
14 mgaleg.maryland.gov/webmga/frmMain.aspx?id=sb0030&stab=01&pid=billpage&tab=subject3&ys=2019rs
15 billstatus.ls.state.ms.us/2019/pdf/history/SB/SB2831.xml
16 gencourt.state.nh.us/bill_status/bill_status.aspx?lsr=923&sy=2019&sortoption=&txtsessionyear=2019&txtbillnumber=SB194
17 www.ilga.gov/legislation/BillStatus.asp?DocTypeID=HB&DocNum=3606&GAID=15&SessionID=108&LegID=120294
18 www.leg.state.nv.us/App/NELIS/REL/80th2019/Bill/6732/Overview


ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

# New era for US privacy laws: California and more

No US federal privacy law is in sight but keep a close eye on California and rapidly expanding enforcement and litigation risks. By **Laura Linkomies**.

The California Consumer Privacy Act (CCPA) will come into effect from 1 January 2020 and be enforceable by California's Attorney General from July 2020. The law, often compared somewhat erroneously with the GDPR, was amended in September and will be implemented through regulations that will be finalised in Spring 2020.

Latham & Watkins lawyers offered invaluable insights into the

*Continued on p.3*

# DP is central to Germany's Facebook competition case

**Stewart Dresner** reports from Brussels on the rationale for the German competition authority's decision on Facebook's abuse of its dominant position.

Personal data plays a key role in data-driven services such as social networks, online search, or so called "digital assistants" which are part of our everyday lives. Global players acquire these data while offering their services at first glance for free. With regard to these strongly data-driven business models, there can be a close link between data protection law and competition law, says Andreas Mundt, President of the

*Continued on p.5*

## Future PL&B Events

- *Balancing privacy with biometric techniques used in a commercial context*, 29 January 2020, Macquarie Group, London. Speakers include Onfido on its use of biometric data and its experience of the ICO's sandbox.
- *Germany's data protection law: Trends, opportunities and conflicts,* 11 March 2020, Covington & Burling, London
- *PL&B's 33rd Annual International Conference*, St. John's College, Cambridge 29 June to 1 July 2020.

privacylaws.com

Issue 162 **DECEMBER 2019**

INTERNATIONAL report

ISSUE NO 162 **DECEMBER 2019**

**PUBLISHER**
**Stewart H Dresner**
stewart.dresner@privacylaws.com

**EDITOR**
**Laura Linkomies**
laura.linkomies@privacylaws.com

**DEPUTY EDITOR**
**Tom Cooper**
tom.cooper@privacylaws.com

**ASIA-PACIFIC EDITOR**
**Professor Graham Greenleaf**
graham@austlii.edu.au

**REPORT SUBSCRIPTIONS**
**K'an Thomas**
kan@privacylaws.com

**CONTRIBUTORS**
**Caleb Skeath and Brooke Kahn**
Covington & Burling LLP, US
**Christopher Docksey**
EDPS and Guernsey Data Protection Authority
**Andin Aditya Rahman**
Assegaf Hamzah & Partners, Indonesia
**Merrill Dresner**
Assistant Editor, *PL&B*

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
**Tel: +44 (0)20 8868 9200**
**Email: info@privacylaws.com**
**Website: www.privacylaws.com**
**Subscriptions:** The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.
Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686
ISSN 2046-844X



# comment

## Privacy developments around the world

We continuously monitor legislative developments globally. In this issue, Professor Greenleaf analyses the situation in Sri Lanka, which now has a GDPR-inspired bill, Pakistan and Nepal (p.22). There are also changes to Indonesia's law (p.17).

In the EU, Slovenia is the only country that has not yet transposed the GDPR into national law. The much-awaited new Greek data protection law entered into force at the end of August and we will publish an analysis of it in the next issue of *PL&B International*. The Greek law implements both the provisions of the EU Law Enforcement Directive and the GDPR.

In the US, the California Consumer Privacy Act (CCPA) will come into effect from 1 January 2020 (p.1) , and there are also changes to US state data breach notification laws (p.10).

How do we keep up with all these developments? Mainly with the help of our knowledgeable correspondents, but also by directly talking to regulators at events such as the DPA's International Conference in Albania (p.7 and p.12), where I met regulators from many countries including Malta's Information and Data Protection Commissioner to learn about Malta's new law (p.20). The host country, Albania, also granted us an interview, the results of which you can see on p.18.

Our own events also play a role. In March we will welcome authoritative speakers from Covington & Burling, Germany to our one-day conference in London on Germany's data protection law, as well as the Head of Department at Bavaria's Data Protection Authority (See programme at www.privacylaws.com/germany).

On p.14, read an analysis of accountability – it is a global standard with great advantages for organisations and regulators, says the author, Christopher Docksey, Honorary Director-General at the EDPS.

To help you in your own research, we have now updated our webpage www.privacylaws.com/links which includes links to 140 national/sub national DPAs, in 97 countries. Also available is online search by keyword to *PL&B's* previous publications and events.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

## Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

# Join the Privacy Laws & Business community

The *PL&B International Report*, published six times a year, is the world's longest running international privacy laws publication. It provides comprehensive global news, on 165+ countries alongside legal analysis, management guidance and corporate case studies.

## PL&B's International Report will help you to:

**Stay informed of data protection legislative developments in 165+ countries.**

**Learn from others' experience through case studies and analysis.**

**Incorporate compliance solutions into your business strategy.**

**Find out about future regulatory plans.**

**Understand laws, regulations, court and administrative decisions and what they will mean to you.**

**Be alert to future privacy and data protection law issues that will affect your organisation's compliance and reputation.**

## Included in your subscription:

**1. Six issues published annually**

**2. Online search by keyword**
Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

**3. Electronic Version**
We will email you the PDF edition which you can also access via the *PL&B* website.

**4. Paper version also available**
Postal charges apply outside the UK.

**5. News Updates**
Additional email updates keep you regularly informed of the latest developments in Data Protection and related laws.

**6. Back Issues**
Access all *PL&B International Report* back issues.

**7. Events Documentation**
Access events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

**8. Helpline Enquiry Service**
Contact the *PL&B* team with questions such as the current status of legislation, and sources for specific texts. This service does not offer legal advice or provide consultancy.

**privacylaws.com/reports**

> "*Privacy Laws & Business* is my go-to for the latest international thought leadership on hot topics in data protection law and policy."
>
> **Giles Pratt, Partner, Freshfields Bruckhaus Deringer LLP**

## UK Report

Privacy Laws & Business also publishes *PL&B UK Report*, covering the Data Protection Act 2018, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Electronic Communications Regulations 2003.

Stay informed of data protection legislative developments, learn from others' experience through case studies and analysis, and incorporate compliance solutions into your business strategy.

## Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

## Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.